REMARKS

Claims 1-22 are pending in the application. Claims have been rejected under 35 U.S.C. 102(e). Those rejections are respectfully traversed and reconsideration is requested.

Claims 1-5, 8-18, 21, and 22 have been amended to more precisely claim the disclosed invention. Support for the amendments can be found in the Applicants' specification on at least page 3, line 25 – page 4, line 3; page 5, lines 5-10; page 6, line 28 – page 7, line 3; page 7, lines 14-20; page 9, line 28 – page 10, line 10; page 13, lines 7-21; and Figs. 1, 2, 3, and 6A-6C.

New Claims 23 and 24 have been added. Support for the new claims can be found in the Applicants' specification on at least page 4, line 29 – page 5, line 2, and page 6, lines 16-21.

Claims 7 and 20 have been canceled.

Thus, Claims 1-6, 8-19, and 21-24 will be pending in the application upon entry of this Amendment, of which, Claims 1 and 17 are independent.

Rejections under 35 U.S.C. 102(e)

Claims 1-6, 8-19, 21, and 22 have been rejected under 35 U.S.C. 102(e) as being anticipated by Belfiore *et al.* (U.S. Patent No. 6,990,513), hereinafter "Belfiore."

Before discussing the cited references, however, a brief review of the Applicants' disclosure may be helpful without limiting the claims. The Applicants' disclosure is directed to a method and system for providing a usage accountability model for data security in a data processing system. Referring to Figs. 2 and 3 of the Applicants' specification, an agent process 300 runs in the background of a client operating system kernel 102 and interrupts requests for access to digital assets (e.g., data files) at a point of authorized access to the assets. The agent process 300 contains sensors 500 that capture low-level (atomic) system events 350, 510, such as file read, file write, clipboard copy, CD-RW access, TCP/IP network message outbound, and the like. The atomic events 350, 510 are then associated with one or more file names, and a filter 520 filters the atomic events 350, 510 against an approved list, removing atomic events that are associated with approved files (such as operating system files) that likely do not contain sensitive application data. A coalescer 530 further processes the atomic events 350, 510 associated with, or related to, a single user action. For example, a typical pattern of file access is a "file open"

atomic event followed by multiple "file read" atomic events to the same file. If such a sequence of atomic events 350, 510 occurs from the same process and the same executable with the same thread ID and the same file name, the coalescer 530 counts the multiple atomic events as only a single "file open" atomic event. The resulting events are then bundled together and sent securely to a journaling server 104-2 that examines the events to determine the occurrence of an aggregate event 360, the presence of which may indicate an abuse of authorized access to the digital asset(s). For example, an aggregate "FileEdit" event may be reported by the journaling server 104-2 if a user has opened and modified a sensitive financial document, with that user then printing the document, renaming it, and saving it to a newly attached USB hard drive.

As illustrated in Figs. 6A-6C, a set of reports are then generated based on the aggregate events, which provide an understanding of how files have been accessed, used, and communicated by various end users of the data processing system. The reports serve as an audit trail that may be used to determine possible abuses of authorized access to the digital assets (e.g., data files).

Turning to the cited reference, Belfiore presents a method and system for facilitating improved communications and collaboration across computer networks consisting of client devices and multiple servers. One particular component of Belfiore is an event component, which is used to synchronize events and provide notification about certain activities within the system. The event component includes an event composition mechanism that transforms atomic level events into progressively higher levels events based on rules, filters, and pattern recognizers. These events (of varying levels) are passed between software components at various locations in the computer network. Upon receiving an event, the receiving software component may perform a particular action based on the received event. For example, the receipt of a certain event may cause an administrator of the network to receive an urgent notification that a server of the network has failed. Also, while Belfiore includes a security component that may control how the events are communicated, it should be stressed that the events of Belfiore are not used to control network security.

Regarding independent Claims 1 and 17, Belfiore does not teach or suggest *"generating an audit trail from the at least one aggregate event, the audit trail representing usage of the at least one digital asset by the end user"* as now claimed in independent Claims 1 and 17. Even if

the event composition mechanism of Belfiore were to be construed as being the equivalent of the aggregator of the present invention, Belfiore passes its events between software components at various locations in the network. When a given software component receives a certain event, the software component may perform a particular task based on the certain event. For example, a software component associated with a teenager using an instant messenger application may receive an event notifying the software component that a friend of the teenager has logged on to the system. In this situation, the software component receiving the event may notify the teenager of the presence of his friend. (*See* Belfiore, col. 4, lines 11-48.)

In contrast, the present invention generates an audit trail from the aggregate messages generated by the journaling server. The audit trail represents usage of particular digital assets of the data processing system of the present invention, and is used to provide an accountability model for security of the system's digital assets, which Belfiore does not disclose. Therefore, because Belfiore does not teach or suggest the audit trail as claimed in independent Claims 1 and 17, and further because the event component of Belfiore is not used to control data security, it is believed that Claims 1 and 17 should be found in condition for allowance.

Dependent Claims 2-6, 8-16, 18, 19, 21, and 22 are directly or indirectly dependent on independent Claims 1 or 17, thus, Applicants respectfully submit that these claims are novel and nonobvious over the cited art for at least the same reasons as presented above for independent Claims 1 and 17.

Furthermore, dependent Claims 2-6, 8-16, 18, 19, 21, and 22 recite further limitations that are neither taught nor suggested by the cited or prior art. For example, regarding Claims 4 and 18, Belfiore does not teach or suggest *"filtering the atomic level events with an approved event list,"* wherein the aggregator only considers *"atomic level events not filtered out by the filter"* as now claimed in Claims 4 and 18. The filter of Belfiore specifies a single event of interest (*see* Belfiore, col. 22, lines 63-66), while the filter of the present invention acts to filter out events that are associated with approved events that do not need to be considered by the aggregator. Nowhere in Belfiore is such a filter disclosed. Applicants note that according to section 2131 of the MPEP, *"[a] claim is anticipated only if each and every element as set forth in the claim is found,"* and that *"[t]he identical invention must be shown in as complete detail as is contained in the ... claim."* Therefore, in addition to the reasons presented above for Claims 1

and 17, because Belfiore discloses no such filter as described in Claims 4 and 18, it is believed that Claims 4 and 18 should be found in condition for allowance.

As a further example, regarding Claims 8 and 21, Belfiore does not teach or suggest *"coalescing at least some of the atomic events into a single event"* as now claimed in Claim 8 and as similarly claimed in Claim 21. In the Applicants' specification coalescing is explained as meaning the combination of a number of related atomic events into a single atomic event, such as, for example, the combination of a "file open" atomic event followed by multiple "file read" atomic events to the same file. This is different than the meaning of event aggregation, as the multiple atomic level events are not aggregated into a higher level event, but coalesced into a single atomic (low level) event. In the above example, the "file open" event and multiple "file read" events will be combined into a single "file open" atomic event. Belfiore discloses no such coalescer. The Office Action cited reference numeral 606 of Fig. 5 as disclosing the Applicants' claimed coalescer, however, reference numeral 606 refers only to the multiple atomic events of Belfiore being sent to Belfiore's event composition mechanism, and not being coalesced in any way. Moreover, the event composition mechanism of Belfiore cannot be construed to be a coalescer as defined in the Applicants' specification, as Belfiore's event composition mechanism combines atomic level event into progressively higher level events and, as explained above, the claimed coalescer does not combine events into higher level events, but into a single event of the same level. Therefore, in addition to the reasons presented above for Claims 1 and 17, because Belfiore does not disclose the coalescing of multiple atomic event into a single atomic event as claimed in Claims 8 and 21, it is believed that Claims 8 and 21 should be found in condition for allowance.

As yet a further example, regarding Claims 14 and 15, Belfiore does not teach or suggest *"control[ling] security of the data processing system by determining patterns of unexpected behavior based on the at least one aggregate event and the audit trail"* or *"provid[ing] a perimeter of accountability for usage of the at least one digital asset"* as now claimed in Claims 14 and 15, respectively. It should be noted that while Belfiore includes a security component that may control how the events of Belfiore are communicated, that the events of Belfiore are not used to control network security. Furthermore, Belfiore does not disclose determining patterns of unexpected behavior based on its events, nor does Belfiore disclose providing a perimeter of

accountability for usage of any of its assets. Thus, because the events of Belfiore are neither used to control security, nor used to determine patterns of unexpected behavior, Belfiore cannot disclose the Applicants' invention as claimed in Claim 14, and because Belfiore does not determine accountability for asset usage outside a perimeter of accountability, Belfiore cannot disclose the Applicants' invention as claimed in Claim 15. Therefore, in addition to the reasons presented above for Claims 1 and 17, because Belfiore does not teach or suggest determining patterns of unexpected behavior or providing a perimeter of accountability, Claims 14 and 15 are believed to be in condition for allowance.

As such, the 35 U.S.C. 102(e) rejections of Claims 1-6, 8-19, 21, and 22 are believed to be overcome. Withdrawal of the rejections under 35 U.S.C. 102(e) is respectfully requested.

New Claims 23 and 24 depend from independent Claims 1 and 17, respectively, and are believed to be in condition for allowance for at least the same reasons as presented above for Claims 1 and 17. Therefore, acceptance of Claims 1-6, 8-19, and 21-24 is respectfully requested.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims that will be pending after entry of this Amendment, Claims 1-6, 8-19, and 21-24, are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By _____

Patrick A. Quinlan
Registration No. 61,287
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133

Date: 11/5/07